jc598 U.S

02/04/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No. AT9-97-308B
Prior Application No.: 08/907,298
First Named Inventor: Ronald Roscoe Bush

Examiner: S. Kabakoff
Art Unit: 2767

jc511 U.S. PTO
09/498293
02/04/00

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir: This is a request for filing a   _____ continuation
                                                      _____ continuation-in-part
                                                      __X__ divisional

application under **37 CFR 1.53(b)**, of pending prior application serial no. 08/907,298, filed on August 6, 1997, for SECURE ENCRYPTION OF DATA PACKETS FOR TRANSMISSION OVER UNSECURED NETWORKS.

1.   __X__   Enclosed is a complete copy of the prior application **including the oath or declaration as originally filed** and an affidavit or declaration verifying it as a true copy. (See No. 14 for declaration.)

2.   _____   New formal drawings are enclosed.

3.   _____   A preliminary amendment is enclosed. (Claims added by this amendment have been properly numbered consecutively beginning with the number next following the highest numbered original claim in the prior application.)

4.   __X__   Also enclosed: Return Postcard

5.   _____   A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 __ is enclosed _____ was filed in the prior application and such status is still proper and desired (37 CFR 1.28(a).

6.   __X__   Cancel in this application original claims 1-14 and 21-20 of the prior application before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

7.   __X__   Amend the specification by inserting the following sentence before the first line: "This is a _____ Continuation, __Continuation-in-Part or __X__ Division of application serial no. 08/907,298, filed August 6, 1997, currently pending."

8.   _____   Priority of application serial No. _____, filed on _____, in _____ is claimed under 35 U.S.C. 119. The certified copy has been filed in prior application serial no. _____, filed _ _____.

9._____X_____The filing fee is calculated below:

CLAIMS AS FILED IN THE PRIOR APPLICATION
LESS ANY CLAIMS CANCELLED BY AMENDMENT NOW

Basic Fee		$690.00
Extra Total Claims (___ x $18.00)	=	0.00
Extra Independent Claims (___ x $78.00)	=	0.00
Total Filing Fee:	=	$690.00

10._____X_____The Commissioner is hereby authorized to charge $690.00 and any additional fee which may be required, or credit any overpayment to IBM Corporation Deposit Account 09-0447. *A duplicate of this sheet is enclosed.*

11._____A check in the amount of $.00 is enclosed.

12._____X_____The prior application is assigned of record to International Business Machines Corporation.

13._____X_____The power of attorney in the prior application is to David A. Mims, Jr. and Andrew J. Dillon.

      a.__X__The power of attorney appears in the original papers in the prior application.
      b._____A new power of attorney is enclosed *(adding prosecution attorneys)*.
      c._____Since the power of attorney does not appear in the original papers, a copy of the power in the prior application is enclosed.
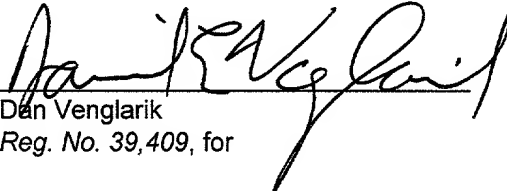   d.__X__Address all future communication to: **Andrew J. DillonVenvlarik,** *Esq.,* **Felsman, Bradley, Vaden, Gunter & Dillon, LLP, Suite 350, Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731**.

14._____X_____I hereby verify that the attached papers are a true copy of prior application serial no. 08/907,298, as originally filed on August 6, 1997.

The undersigned declares further that all statements made herein of his or her own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application of any patent issuing thereon.

_____February 4, 2000_____
Date

Address of signatory:
FELSMAN, BRADLEY, VADEN,
  GUNTER & DILLON, LLP
201 Main Street, Suite 1600
Fort Worth, Texas 76102
817/332-8143

Dan Venglarik
Reg. No. 39,409, for

_____ Inventor(s)
_____ Assignee of complete interest
_____ Attorney or agent of record
___X___ Filed under §1.34(a)

Attorney Docket No. AT9-97-308B

SECURE ENCRYPTION OF DATA PACKETS FOR TRANSMISSION OVER UNSECURED NETWORKS

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates in general to data encryption and in particular to securing data transfers over unsecured channels of communications. Still more particularly, the present invention relates to practical implementation of unbreakable data encryption through one-time use of pure random numbers.

2. Description of the Related Art:

Sensitive data transfers are increasingly occurring over networks which are unsecured, such as the Internet or cellular telephone networks. By their nature, the medium by which data transfers are made in such networks must be openly accessible and/or shared, leaving transactions susceptible to interception. The only available alternative for securing data transfers over such networks thus becomes data encryption.

A variety of data encryption schemes have been developed and are implemented for data transfers over networks of the type described. For example, many data encoding schemes employ a reversible encryption algorithm modeled after the Data Encryption Standard (DES). Other data encoding schemes, used alone or in conjunction with DES, employ a combination of public and private keys to encrypt data, such as the Rivest-Shamir-Aldeman (RSA) encryption system used in many commercial software packages. These encoding schemes utilize pseudo-

random numbers, or number sequences having a high degree of randomness.

The only encryption system currently recognized as being unconditionally secure is the "one-time pad," also known as a Vernam cipher, developed by Gilbert S. Vernam while working for AT&T in 1917. When properly implemented, the one-time pad encryption mechanism is generally recognized by cryptographic experts to be the only known unbreakable encoding scheme. Other encryption systems are considered cryptographically secure, meaning that the costs associated with breaking the code by pure mathematical methods and extensive computation are very high, although the code can theoretically be broken if enough computing power could be brought to bear. One-time pads are unconditionally secure, meaning that any amount of analysis and computing power is insufficient because there is no pattern in the data.

The two key characteristics of the one-time pad concept which must be adhered to for encryption with a one-time pad to be unconditionally secure are pure randomness and one-time use. Pure randomness is thought to occur in the timing of radioactive decay and in the arrival of cosmic background radiation. The present invention employs one or both of the above sources passed through a cryptographically strong one-way function as the source of random values. Furthermore, the present invention requires that the random sequences thus generated are never intentionally used in more than one embodiment.

Although recognized as being mathematically unbreakable, the one time pad is conventionally considered not to be

commercially practical. The reason is principally conven-
ience, since the security of the system requires that the
contents of the one-time pad be known only to the proper
encrypting and decrypting entities. This requires secure
distribution of the one-time pads. Furthermore, the one-time
pad, when properly employed, requires large amounts of pure
random data for the encryption/decryption values which, by
definition, may be used only once. Additionally, since the
one-time pad contains only a finite number of random numbers
for encryption, replacement of the one-time pad is inevitably
required. Finally, the one-time pad encryption method is less
ideally suited for encryption of long, variable length
messages than alternative, less secure encryption schemes.
For these reasons, one-time pads have not been employed up to
this time in actual encryption systems for commercial
applications, such as banking, cellular telephony, etc.

There do exist classes of problems, however, for which
the one-time pad could provide unconditionally secure
encryption on a commercial basis. It would be desirable,
therefore, to provide a method and apparatus for employing
one-time pads in commercial applications requiring encryption
of data for transfer over unsecured networks. It would
further be advantageous to provide an implementation of one-
time pads which could be readily adapted to a variety of
commercial data encryption requirements.

SUMMARY OF THE INVENTION

It is therefore one object of the present invention to provide an improved method and apparatus for data encryption.

It is another object of the present invention to provide an improved method and apparatus for securing data transfers over unsecured channels of communications.

It is yet another object of the present invention to provide practical implementation of unbreakable data encryption through one-time use of pure random numbers.

The foregoing objects are achieved as is now described. Pure random numbers from a sheet within a one-time pad are employed to encrypt the bytes of a source data packet and to order the encrypted bytes in a random order within the encrypted data packet. Pure random numbers fill remaining positions within the encrypted data packet. The resulting encrypted data packet is unconditionally secure (i.e., unbreakable). Sheets within the one-time pad are utilized only once, and the one-time pad is replaced when exhausted. For electronic checking applications, the one-time pad is distributed to the user stored in an electronic checkbook, with a copy retained by the bank. For cellular telephone applications, the one-time pad is stored in a replaceable memory chip within the mobile unit with a copy retained at a single, secured central computer. For client-server applications or applications involving sales over the Internet, the one-time pad may be provided to the user on a floppy disk or CD-ROM, with a copy retained by the vendor.

The above as well as additional objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a block diagram of a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 2 is a diagram of the contents of a sheet within a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 3 depicts an example of data encryption utilizing a one-time pad in accordance with a preferred embodiment of the present invention;

Figure 4 is a high level flowchart for a process of encrypting data in accordance with a preferred embodiment of the present invention;

Figure 5 depicts a high level flowchart for a process of decoding data in accordance with a preferred embodiment of the present invention;

Figure 6 is a diagram of an electronic checking environment in which secure encryption in accordance with a

preferred embodiment of the present invention may be implemented;

Figure 7 depicts a data flow diagram for a process of utilizing electronic checks in accordance with a preferred embodiment of the present invention;

Figure 8 is a block diagram of a cellular communications global transponder in which a preferred embodiment of the present invention may be implemented; and

Figure 9 depicts an Internet sales environment in which a preferred embodiment of the present invention may be implemented.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures, and in particular with reference to **Figure 1**, a block diagram of a one-time pad in accordance with a preferred embodiment of the present invention is depicted. One-time pad **102** is maintained in a memory, such as a read only memory (ROM) or a hard disk drive, and includes a plurality of sheets **104**. Each sheet **104** contains a plurality of pure random numbers sufficient for encryption of a known, fixed length (N) data packet. Each sheet **104** is not intentionally used in the implementation of any other one-time pads such as one-time pad **102**.

Referring to **Figure 2**, a diagram of the contents of a sheet within a one-time pad in accordance with a preferred embodiment of the present invention is illustrated. Each sheet **104** contains a string **202** of N pure randomly-ordered numbers in the range of 1 to N. Each sheet **104** also contains a plurality of corresponding arrays **204**. Number string **202** is a non-repeating sequence of numbers within the predetermined range N corresponding to the number of characters or positions in the encrypted data packet. For example, if the encrypted data packet will have five hundred positions, the numerals 1 through 500 will be randomly ordered and placed in string **202**. Individual numbers within string **202** are employed to identify the position for a corresponding byte of data in the encrypted data packet. For example, the first number **206** within string **202** designates the position within the encrypted data packet in which the first byte of source data will be placed after encryption.

Each individual number within string **202** has an

associated array within array set **204**.   Each array **208** contains a non-repeating sequence of random numbers comprising a character map to be employed for the character in the respective position.   For the sake of simplicity and clarity of explanation, the exemplary embodiment depicts only the mapping for numeric characters 0-9 and a delimiter ("*"). However, the mapping may easily be extended to include alphabetic or text characters merely by increasing the size of arrays **204**.   The arrays **204** essentially comprise encryption instructions for data packets not exceeding the length of position string **202**.

The characters or values within a character map array **208** for a given position are randomly generated subject only to the constraint that the same value may not appear twice in a given array.   However, the same value may appear many times within different arrays in array set **204**.   In fact, 128 different characters can be encoded in each byte comprising map array **208**.   While the exemplary embodiment depicts only numerals less than 100 in arrays **204**, any set of 128 unique characters may be employed to form the character maps, including alphanumeric characters and special characters (colons, hyphens, dashes, quotation marks, punctuation, etc.).

The fact that only 128 different characters can be represented within any one byte of array **208** creates a limitation on the encryption of double byte based text that occurs in Asian languages. However, the present invention is likely to find its widest commercial use in short, fixed length, numeric related applications such as electronic checking, position reporting, and client-server authentication and verification. Since the present invention is not intended

for widespread use in text encryption, the exemplary embodiment illustrates a single byte approach. However, those skilled in the art will quickly understand that the present invention can be extended to include double byte encoding.

5

As described, the character map values within each array 208 in array set 204 are random numbers, and the sequence of numbers in string 202 is randomly ordered. Two sources of "randomness" are thought to exist: the time period associated with electronic emission/decay for a single radioactive particle and the level of background radiation originating from space. Methods for generating pure random numbers are well-known in the art, and include measuring the random time intervals associated with radioactive decay or cosmic background radiation and passing these measurements through a one-way hash function. These methods may be employed in known manners for generating values for the character maps in arrays 204, for randomly ordering numbers within string 202, and for filling the unused bytes of the encrypted data packet.

Referring again to **Figure 1**, the requirement that true random numbers be employed in sheets 104 within one-time pad 102 cannot be circumvented for convenience. Pseudo-random numbers, which are usually generated from a seed value using a hash function, are not acceptable substitutes since an estimate of the seed value may be employed to derive the hash function required to duplicate the resulting pattern. With a fairly accurate estimate of the seed value, the number of mathematical operations required to crack the encryption mechanism becomes workable. The vulnerability of pseudo-random numbers, even those believed to be cryptographically secure, has been demonstrated where the time and process id

have been used in the key of popular software security
features.

One-time pad **102** may also include counter **106** identifying
the next sheet **104** which may be utilized for encryption or
decryption. Both the encrypting and decrypting entities are
provided with identical copies of one-time pad **102** through a
secure medium such as hand-delivery. As sheets **104** within
one-time pad **102** are utilized, counter **106** is advanced to
point to the next available sheet. When counter **106** contains
a value exceeding the number of sheets **104** within one-time pad
102, one-time pad **102** is depleted and must be replaced.

The requirement that a given sheet **104** within one-time
pad **102** be used only once and never be reused is critical.
Reuse of sheets **104** within one-time pad **102** compromises the
security of the resulting encrypted data packet. It is
intended that data packets encrypted by the method provided in
the present invention could be accompanied by the plain text
of the source packet, and still be invulnerable to crypto-
graphic attack. Reuse of sheets **104** would prohibit this level
of unconditionally secure encryption.

With reference now to **Figure 3**, an example of data
encryption utilizing a one-time pad in accordance with a
preferred embodiment of the present invention is depicted.
Source data packet **302** contains a string of characters
comprising the message to be encrypted for transmission.
Again, while the exemplary embodiment depicts only numeric
characters and a delimiter, the process described may be
readily applied to expanded character sets.

Furthermore, the order in which the pure random numbers are used from sheet **104** within a specific one-time pad **102** can be varied depending on a particular customer or implementation. The same encoding/decoding software is simply placed

5   in the one-time pad device and the decoding computer. This allows for further security through the ability to physically secure the one-time pad and the encoding/decoding software separately. The ability to separate responsibilities is one key method used in the prevention of theft by inside

10   employees. In the exemplary embodiment, one particular pattern is followed for illustrative purposes.

The encrypted data packet **304** contains positions for the encrypted bytes of source data packet **302**, with five hundred positions depicted in the exemplary embodiment. The value of

15   the first numeral in the position string of a sheet in the one-time pad is utilized to determine the position of the first encrypted byte. Utilizing the example depicted in **Figure 2**, the first encrypted byte of source data packet is to be placed in position 3. The value of the first byte within

20   source data packet is looked up in the associated character map for position 3, and the encrypted value "92" is entered in encrypted data packet **304** at position 3. Similarly, the value "67" is entered in position 14 and the value "38" is entered

25   in the ninth position of encrypted data packet **304** to encode the second and third bytes of source data packet **302**, respectively. This encryption process continues until all bytes of source data packet **302** have been encrypted.

30   When all bytes of source data packet **302** have been processed and an encryption value placed in the appropriate position of encrypted data packet **304**, the remaining positions

are filled. The remaining positions may be filled with pure random numbers from the sheet of the one-time pad being employed. The positions within the encrypted data packet **304** which do not contain values from the source data packet **302** are used for authentication, verification, and disinformation.

When expanded to include the full character set, the secure encryption mechanism of the present invention possesses the ability to randomly encode each byte of a source data packet in at least 128 different ways. Furthermore, any character of data may be placed in any of the positions within the encrypted data packet. Thus, each character of data may be encrypted in hundreds of thousands of different ways, depending on the length of the encrypted data packet, with each character entirely independent of any other character. There exists no pattern in either the encoding of a character or its position within an encrypted data packet, nor is there any pattern between distinct encrypted data packets. The encoding and position mappings are known only to entities possessing a copy of the one-time pad and knowing which sheet was employed for encryption. No human intervention is required for either the random number generation, encoding, or decoding processes. Once a sheet within the one-time pad has been used, that sheet is never intentionally used again, although theoretically the same sheet may be randomly generated again within another one-time pad.

The feature of randomly ordering encrypted byte within the encrypted data packet is not found in conventional one-time pads, which are simple look-up tables for each character or word placed in order in the encrypted message. Thus, the present invention provides greater security than conventional

one-time pads. Furthermore, the starting location for the position string and arrays may be varied from one-time pad to one-time pad. For example, one one-time pad may begin with the fifth numeral in the position string, while another begins with the fifty-third numeral.

It should be noted that the "arrays" described above are simple constructs used for convenience in describing the invention. Other methods of employing random numbers to encrypt the source data may be employed instead of or in addition to character maps, including XORing the bits of a random number with the bits of the character or word being encrypted.

Referring to **Figure 4**, a high level flowchart for a process of encrypting data in accordance with a preferred embodiment of the present invention is illustrated. The process begins at step **402**, which depicts initiation of the encryption process by a transmitting entity preparing to transmit a source data packet over an unsecured network. The process then passes to step **404**, which illustrates reading a sheet from the one-time pad and, if the one-time pad is equipped with a counter, incrementing the counter.

The process next passes to step **406**, which depicts reading a position indicator from the positions string, and then to step **408**, which illustrates reading the next character to be encrypted from the source data packet. The process passes next to step **410**, which depicts looking up the character to be encrypted in the character map associated with the position identified by the position indicator. The process then passes to step **412**, which illustrates placing the

encrypted character associated in the character map with the character read from the source data packet in the position designated by the position indicator read from the position string.

The process then passes to step **414**, which depicts a determination of whether the entire source data packet has been encrypted. If not, the process returns to step **406** for encryption of additional characters from the source data packet as described above. If so, however, the process proceeds to step **414**, which illustrates filling the remaining positions in the encrypted data packet. As described above, the remaining positions may be filled with information encrypted with pure random numbers for authentication, verification, or disinformation purposes.

Once the entire encrypted data packet is filled, the process passes to step **416**, which depicts the process becoming idle until another data packet requires encryption. The data packet encrypted by the process described may be securely transmitted over unsecured networks without danger of being compromised.

With reference now to **Figure 5**, a high level flowchart for a process of decoding data in accordance with a preferred embodiment of the present invention is illustrated. The process begins at step **502**, which depicts initiation of the decryption process in response, for example, to receipt of an encrypted data packet. The process then passes to step **504**, which illustrates reading the next available sheet from the one-time pad and, if the optional counter is present, incrementing the counter.

The process next passes to step **506**, which depicts reading the first (or next) position in the position string within the one-time pad sheet, and then to step **508**, which illustrates reading the encrypted character at the position within the encrypted data packet designated by the position indicator read. The process passes next to step **510**, which depicts looking up the encrypted character in the character map associated with the designated position to determine the decoded character. The process then passes to step **512**, which illustrates placing the decoded character in the next available position within the decoded data packet.

The process then passes to step **514**, which depicts a determination of whether the encrypted data packet has been completely decoded. This determination may be made, for example, based on whether an expected number of characters have been decoded from the encrypted data packet, or on whether a stop character and expected fill characters have been encountered. If further decoding is required, the process returns to step **506** for decryption of additional characters within the encrypted data packet.

A determination of whether the decode was successful may simply involve checking the decoded data packet for a stop character, checking for a known number of characters to be decoded, or may involve looking for an expected authentication or verification character sequence ("watermark" or "signature") within the decoded data packet. When the message has been decoded, the fill characters are checked for authentication and verification purposes.

If the decode was not successful, the process may

optionally proceed to step **518**, which illustrates adjusting the one-time pad employed in the decryption process in an attempt to resynchronize the one-time pads employed by the transmitting and receiving entities. This may be achieved, for example, by adjusting the counter value to compensate for the receiving entity being behind the transmitting entity, the most likely source of error in synchronization. If the counter was incremented in the last decryption attempt, the decrypting process may simply be attempted again.

To avoid the potential for synchronization errors in utilizing sheets within the one-time pad, an alternative procedure is to have the decryption process check the fill characters in adjacent sheets for authentication and verification purposes prior to decoding.

Referring again to step **516**, if the data packet was successfully decoded, the process proceeds instead to step **520**, which depicts the process becoming idle until decryption of a received data packet is once again required.

Referring to **Figure 6**, an electronic checking environment in which secure encryption in accordance with a preferred embodiment of the present invention may be implemented is depicted. The electronic checking environment depicted includes a receiving device **602** located at the merchant's place of business which is connected to a server **604** located at the customer's bank. Receiving device **602** may be connected via communications link **606** to the Internet **608**, which is in turn connected via communications link **610** to server **604**, such that electronic checks are processed via the Internet. Alternatively, receiving device **602** may be directly connected

to server **604** via communications link **612**, which may provide dial-up access or the like.

An electronic checkbook **614** is capable of being selectively attached to receiving device **602**. The term "electronic checkbook" is used herein to refer to a collection of fixed length randomly encoded data packets, regardless of the medium in which such packets are held, together with the instructions for encrypting. Similarly, the term "electronic check" is used herein to refer to a single fixed length randomly encoded data packet encrypted utilizing the corresponding sheet from a one-time pad. Each electronic check within an electronic checkbook is utilized only once.

The electronic checks generated by electronic checkbook **614** would contain, in an encrypted data packet, information such as the amount, the payee's account number, and the customer's signature. The signature may comprise a simple password, or may be a fingerprint, retina scan, or any other positive means of identification. The number of bytes required to encode a check's confidential information should be on the order of 100 bytes, although each electronic check may be on the order of a few hundred bytes with the unused bytes filled with additional characters as described above.

When an individual first becomes a customer of a bank, or reorders checks, the bank supplies the customer with electronic checkbook **614**, with bank routing and account identification associated with the electronic checks. Electronic checkbook **614** may include a reorder form for automatic reorder when the number of remaining checks falls below a certain number. The customer may select a password or

personal identification number (PIN), i.e., signature, to be associated with the electronic checks as is currently done for automated teller machine (ATM) access.

5   The collection of data packets comprising electronic checkbook **614** are contained within a suitable form of electronic memory encased in a hard case or other suitable durable means of protecting the memory. The electronic checkbook **614** may be a simple memory device such as a type of
10   Personal Computer Memory Card International Association (PCMCIA) card capable of being inserted into receiving device **602**. Receiving device **602** may thus be equipped with a keyboard and display (not shown) for user interaction and the capability of reading electronic checks from electronic
15   checkbook **614**, encrypting transaction information utilizing the associated sheet from a one time pad, and transmitting the encrypted data packet for the transaction while deleting the one-time pad sheet from any local or internal memory in receiving device **602**. For additional security, the encryption
20   could occur only within the PCMCIA card. However, this method allows for the possibility of the checkbook owner's password being compromised, which is not the preferred embodiment of the present invention.

25   Alternatively, in the preferred embodiment of the present invention, electronic checkbook **614** could be a relatively simple device allowing for write-only transmission of encrypted data packets. That is, no capability to read its contents would exist. A small keyboard, a small display, and
30   a single port would be required, with electronic checkbook **614** inserted into receiving device **602** when preparing to write an electronic check. Receiving device **602** may be located at the

merchant's place of business or be connected to a customer's computer for transactions over the Internet. The payee and the amount could be automatically provided by receiving device **602**, with the customer entering a password and pressing a write button when the correct payee and amount are displayed. The electronic check would then be written to receiving device **602**, which would transmit the electronic check to server **604** for processing.

As still another alternative, electronic checkbook **614** may be downloaded into a device possessed by the customer, such as a personal digital assistant (PDA). Electronic checkbook **614** could be downloaded to the customer's PDA at the time the account is opened, with checks replenished without human interaction at ATM's modified to include a port for this purpose. Therefore, check replenishment would be readily available 24 hours a day.

Server **604** located at the customer's bank is connected to a storage device **616** containing the other copy of the one-time pad utilized to encrypt the confidential information within the electronic check and an authorized check list associating electronic checks with sheets of the one-time pad. The electronic checking environment may also include a second server **618** located at the payee's bank connected to Internet **608** by communications link **620**, and a third server **622** located at a clearinghouse connected to Internet **608** via communications link **624**. In this manner, the electronic checks may be passed among all entities concerned via Internet **608** without generating any paper.

By encrypting the electronic checks using a one-time pad

in accordance with the present invention, the plain text of
at least a portion of the encrypted message--such as the
amount, the payee, etc.--may accompany the encrypted
electronic check and the encrypted data would still be
invulnerable to cryptographic attack. Knowledge of a portion
of the message encrypted, even if accompanied by knowledge of
the ordering of these portions within the source message, is
of no benefit in attempting to break the encrypted message.
Thus, authentication and verification codes required to
validate the electronic check would remain encrypted in an
unbreakable manner.

An additional level of security may be introduced by
varying the starting location used for the position string
between electronic checkbooks (i.e, starting with the seventh
random number in the string in one electronic checkbook while
starting with the thirty first random number in a different
electronic checkbook). The responsiblity for generating the
random numbers for the one-time pad may thus be separated from
the responsibility for selecting a starting location within
the position string and arrays to be employed by a particular
one-time pad, increasing the difficulty of employee theft of
the information. An electronic checkbook may be manufactured
and filled with one-time sheets by one entity, and programmed
with a randomly selected starting location within the position
string by a different entity.

With reference now to **Figure 7**, a data flow diagram for
a process of utilizing electronic checks in accordance with a
preferred embodiment of the present invention is depicted.
The merchant or payee supplies the merchant's account
identification and an amount to the payor through a receiving

device. The electronic check, an encrypted data packet such as described above, is generated by the customer or payor **702** and transmitted to the merchant or payee **704**. Merchant **704** appends the merchant's bank routing and account identification

5   numbers to the electronic check, then routes the electronic check to both the payor's bank **706** and the merchant's or payee's own bank **708**.

Payor's bank **706** is the only place where the electronic

10   check can be decoded. When payor's bank **706** receives the electronic check, payor's bank **706** decodes the electronic check, verifies and authenticates the check, checks the balance of the payor's account, freezes the amount indicated in the electronic check within the payor's account, and

15   electronically forwards the electronic check, with the appended payee account information, to clearinghouse **710** together with a coded authorization for payment of the indicated amount to the payee.

At the same time, when payee's bank **708** receives the

20   check, payee's bank **708** marks the payee's account as pending receipt of a deposit and forwards the check to clearinghouse **710**. Clearinghouse **710** compares the two (encrypted) electronic checks received from payor's bank **706** and payee's

25   bank **708**. If they match, clearinghouse subtracts the indicated amount from the clearing account of payor's bank **706**, adds the indicated amount to the clearing account of payee's bank **708**, notifies payor's bank **706** that the electronic check has been settled, and notifies payee's bank

30   **708** that the electronic check has been settled with the indicated amount placed in the clearing account of payee's bank **708**.

On receipt of the notice from clearinghouse **710**, payor's bank **706** subtracts the indicated amount from the payor's account, removes the electronic check from the payor's authorized check list, and notifies the payor **702** that the check has been settled. The payor's electronic checkbook may then remove the used electronic check from the set of available electronic checks. Meanwhile, on receipt of the notice from clearinghouse **710**, payee's bank **708** adjusts the payee's account by the indicated amount and notifies payee **704** that the check has been settled.

At this point, the transaction is complete. The elapsed time for the transaction could be very short. Bottlenecks will occur primarily from limited bandwidth at the retail counter and within the Internet. Bandwidth problems at the retail counter may be alleviated by using parallel receiving devices.

Use of electronic checks over the Internet, directly from a customer's home, would operate in a similar fashion. However, the customer must send a copy of the electronic check to the merchant. Moreover, a number of additional features could be added to the electronic checking system, such as the ability to directly deposit electronic checks to and/or through the customer's electronic checkbook.

The electronic checking environment of the present invention would allow the current, paper-based checking system to be electronically emulated, while providing greater security than that available in the current paper process. The ease of understanding and heightened security will facilitate earlier and faster adoption of electronic checking.

The current clearinghouse function will persist in an electronic form, and current banking laws, regulations, and procedures may be applied. The present invention also allows paper checks and electronic checks to coexist during a transition period to pure (or majority) electronic banking.

Referring to **Figure 8**, a block diagram of a cellular communications global transponder in which a preferred embodiment of the present invention may be implemented is illustrated. Global transponder **802** is a device which automatically returns a data packet containing the latitude and longitude of the location of global transponder **802** in response to receiving a cellular telephone call. The data packets may be transmitted over non-secure, commercial cellular phone circuits such as those provided by the Iridium Project, which provides global cellular communications to and from any spot on earth.

Global transponder **802** includes processor **804** connected to memory **806**. The connection may be in the form of a system bus **808**, which is also connected to an external port **810** for programming or communication with other devices. Processor **804** is also connected to cellular modem **812**, which is connected in turn to antenna **814**. Processor **804** and antenna **814** are also both connected to global positioning system (GPS) chip set **816**. Such GPS chip sets are available from a number of commercial sources. GPS chip set **816** preferably returns GPS fix data in the NMEA-0183 ASCII RS232 format. Sensors **818** and switches **820** connected to processor **804** provide sources of data and control, respectively, for global transponder **802**.

Global transponder **802** automatically returns a data

packet in response to a cellular phone call from a central
computer (not shown). The content of the data packet that is
returned varies depending on the content of the request packet
originating from the central computer. In general, the data

5   packet returned will include GPS latitude and longitude
information, and may also include sensor data and/or
information regarding the object to which global transponder
802 is attached.

10   When a cellular phone call is received, modem **812**
automatically answers and receives the request packet,
transmitting the request packet to processor **804**. Processor
804 examines the request packet and determines what response
packet should be sent. GPS fix data from GPS chip set **816** is

15   stored in memory **806**, as is data from sensors **818**. Processor
804 extracts the appropriate information from memory **806** for
the response packet, forwarding the response packet to modem
812 for transmission. Although the latitude and longitude may
be transmitted in approximately 20 digits, the data packets

20   returned may be any fixed length. The data packets could
easily be a few hundred bytes long and still be transmitted,
in burst mode, in a very short time interval (on the order of
one second).

25   There are times when the data packets returned by global
transponder **802** must be protected, as in the case of a downed
military pilot. Therefore, the one-time pad of the present
invention may be employed to encrypt the data packet. A
portion of memory **806** may be a microchip containing the one-

30   time pad. When the latitude/longitude of global transponder
802 is required, the central computer dials cellular phone
number of global transponder **802** and transmits a request

packet comprised of a previously determined pattern of random characters. Processor **804** compares the pattern in the request packet to patterns associated with valid sheets of the one-time pad, copies of which are only in global transponder **802** and the central computer.

If processor **804** fails to identify a match with patterns associated with the one-time pad, then global transponder **802** simply terminates the cellular telephone connection without returning a data packet. Global transponder **802** may also record the date and time of the attempted contact. On the other hand, if a match to the pattern in the request packet is determined, processor **804** generates a data packet containing the latitude and longitude encrypted using the sheet of the one-time pad which is associated with the pattern from the request packet. This data packet is then returned to the requesting entity (i.e., the central computer).

Upon receiving the encrypted data packet, the central computer validates the packet by comparing bytes not containing latitude/longitude information with bytes expected to be returned in response to the request packet. If the packet is valid, the central computer extracts and decodes the encrypted latitude and longitude information.

In order to prevent jamming by repeatedly calling the phone number utilized by global transponder **802**, it may be desirable to associate a unique phone number with each sheet in the one-time pad. Thus, global transponder **802** would respond to any of the phone numbers associated with sheets in its one-time pad. In addition, for military applications, buttons may be added to allow a downed pilot to indicate

his/her physical condition, the state of enemy activity, and whether his/her capture is imminent. The sensors might be used to transmit the pilot's vital signs, such as heart rate. Additionally, functionality may be added to allow the pilot to transmit the information without waiting for an incoming cellular phone call, or to indicate whether the device had fallen into enemy hands.

Since the one-time pad and the cellular phone numbers are hard-coded into memory **806** of global transponder **802**, this information cannot be leaked and reverse engineering would not yield any substantive information. The use of commercial connections reduces the cost while providing, with encryption, the same or a better level of security. Fly-overs would not be required since the pilots exact location could be identified, reducing the potential for conflict or compromise of the pilot's location.

With reference now to **Figure 9**, an Internet sales environment in which a preferred embodiment of the present invention may be implemented is depicted. The Internet sales environment includes a user unit **902** connected to the Internet **904** by communications link **906**, which may for example be access through an Internet service provider (ISP). A server **908**, which may be a HyperText Transmission Protocol (HTTP) server, is located at the vendor's facilities and is also connected to Internet **904** via communications link **910**. User unit **902** may include a browser, an application designed to submit HTTP requests and display information formatted in the HyperText Markup Language (HTML). Thus, transactions in the Internet sales environment depicted may be conducted over the World Wide Web (WWW).

The vendor may provide a one-time pad to potential customers. For example, a company selling software may provide a one-time pad to a customer setting up an account to order upgrades or new products over the Internet. Alternatively, the user's credit card company may provide a one-time pad for use in conducting transactions over the Internet. Sales orders transmitted over the Internet **904**, or at least confidential information within sales orders, are encrypted by user unit **902**, and are either decoded by the vendor, if the one-time pad originated from the vendor, or forwarded by the vendor to the credit card company for decoding and payment authorization.

Alternatively, the one-time pad may be employed in client-server environments for authentication and verification purposes. In this alternative, a vendor might be able to deliver software customized for a particular environment after receipt of a data packet encrypted using a one-time pad previously sold to the customer.

It is important to note that while the present invention has been described in the context of fully functional systems, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally regardless of the particular type of signal bearing media used to actually carry out the distribution. Examples of computer readable media include: recordable type media such as floppy disks and CD-ROMs and transmission type media such as digital and analog communication links.

    While the invention has been particularly shown and
described with reference to a preferred embodiment, it will be
understood by those skilled in the art that various changes in
form and detail may be made therein without departing from the
5   spirit and scope of the invention.

CLAIMS:

What is claimed is:

1   1.   A method of encrypting data packets, comprising:

2   selecting a byte within a source data packet;

3   randomly selecting an available position within an

4 encrypted data packet in which to place an encrypted byte

5 corresponding to said selected byte of said source data

6 packet;

7   encrypting said selected byte using a random number to

8 generate said encrypted byte; and

9   placing said encrypted byte in said selected position

10 within said encrypted data packet, wherein said selected byte

11 of said source data packet is encrypted in an unconditionally

12 secure manner.

2.   The method of claim 1, further comprising:

        repeating said steps of selecting a byte, randomly

selecting an available position, encrypting said selected

byte, and placing said encrypted byte in said selected

position for each byte within said source data packet.

1   3.   The method of claim 2, further comprising:

2   after encrypting all bytes of said source data packet,

3 filling remaining positions within said encrypted data packet

4 with random numbers.

1   4.   The method of claim 2, further comprising:

2   after encrypting all bytes of said source data packet,

3 encrypting authentication data; and

4   placing bytes of said encrypted authentication data in

5 remaining positions within said encrypted data packet.

1   5.   A one-time pad, comprising:

2   a memory device;

3   a nonrepeating, randomly ordered sequence of N numbers

4   within the range of 1 to N within the memory device; and

5   a plurality of arrays of random numbers within said

6   memory device, each array within said plurality of arrays

7   associated with a number within said sequence of numbers.

1   6.   The one-time pad of claim 5, wherein each array within

2   the plurality of arrays comprises a character map.

1   7.   The one-time pad of claim 5, wherein said sequence and

2   said plurality of arrays comprise a sheet.

1   8.   The one-time pad of claim 5, further comprising:

2   a counter within said memory device, said counter

3   pointing to a sheet within a plurality of sheets within said

4   one-time pad.

1   9.   An electronic checkbook, comprising:

2   a memory containing a plurality of encryption sheets,

3   each encryption sheet within the plurality of encryption

4   sheets including:

5   a string of N numbers within the range of 1 to N

6   arranged in a nonrepeating, randomly ordered sequence;

7   and

8   a plurality of random number arrays, each array

9   within said plurality of arrays associated with a

10   different number within said string of numbers; and

11   a plurality of identifiers associating each encryption

12   sheet within the plurality of encryption sheets with an

13   electronic check.

1   10. The electronic checkbook of claim 9, wherein each
2   encryption sheet and said associated identifier comprises an
3   unused electronic check.

1   11. The electronic checkbook of claim 9, wherein said
2   electronic check comprises information encrypted using an
3   encryption sheet within said plurality of encryption sheets.

1   12. The electronic checkbook of claim 11, wherein said
2   electronic check further comprises:
3   a plurality of encrypted bytes generated from a plurality
4   of source bytes,
5   wherein each encrypted byte is placed in a position
6   within said plurality of encrypted bytes identified by a
7   position number located within said string at a location
8   corresponding to a location within said plurality of source
9   bytes containing a source byte utilized to generate said
10   encrypted byte, and
11   wherein each encrypted byte comprises a random number
12   corresponding, within an array associated with said position
13   number, to said source byte.

1   13. The electronic checkbook of claim 12, wherein said
2   electronic check further comprises:
3   authentication data encrypted with said plurality of
4   encrypted bytes.

1   14. The electronic checkbook of claim 9, wherein said
2   electronic checkbook further comprises:
3   a port for connection to a receiving device.

1   15. A method of processing an electronic check, comprising:

2   receiving an electronic check encrypted using a one-time

3   pad at a business;

4   transmitting a first copy of said electronic check to a

5   payor's bank and a second copy of said electronic check to a

6   payee's bank; and

7   decoding said first copy of said electronic check at said

8   payor's bank using a copy of said one-time pad.

1   16.   The method of claim 15, further comprising:

2   authenticating said electronic check; and

3   transmitting said first copy of said electronic check to

4   a clearinghouse with a payment authorization.

1   17.   The method of claim 16, further comprising:

2   transmitting said second copy of said electronic check to

3   said clearinghouse;

4   comparing said first copy of said electronic check to

5   said second copy of said electronic check; and

6   responsive to determining that said first copy of said

7   electronic check matches said second copy of said electronic

8   check, processing a transaction transferring funds from said

9   payor's bank to said payee's bank.

1   18.   A method of securing transmission of a global transponder

2   location, comprising:

3   receiving a request packet via a cellular communications

4   link to said global transponder;

5   encrypting a data packet containing a latitude and a

6   longitude for a location of said global transponder using a

7   one-time pad containing within said global transponder; and

8   transmitting said encrypted data packet to a central

9   computer over said cellular communications link.

1   19. The method of claim 18, wherein said step of encrypting

2   a data packet further comprises:

3   locating an identifier within said request packet;

4   comparing said identifier to a plurality of identifiers

5   in said global transponder, wherein identifier within said

6   plurality of identifiers is associated with a sheet within

7   said one-time pad;

8   responsive to determining that said identifier within

9   said request packet does not match any identifier within said

10   plurality of identifiers, terminating said cellular

11   communications link; and

12   responsive to determining that said identifier within

13   said request packet matches an identifier within said

14   plurality of identifiers, encrypting said data packet using a

15   sheet within said one-time pad associated with said matching

16   identifier.

1   20. A global transponder, comprising:

2   a processor connected to a memory containing a one-time

3   pad;

4   a cellular modem connected to said processor and an

5   antenna;

6   a GPS chip set connected to said processor and said

7   antenna, said GPS chip set providing GPS fix data to said

8   processor,

9   wherein said processor, responsive to receiving a call

10   through said cellular modem, encrypts said GPS fix data using

11   said one-time pad for transmission via said cellular modem.

1   21. A method of encrypting data packets using a one-time pad,

2   comprising:

3   selecting a character within a source data packet;

4   reading a position number within a randomly ordered,
5   nonrepeating sequence of N numbers within the range of 1 to N,
6   wherein said position number is at a location within said
7   sequence corresponding to a location of said selected
8   character within said source data packet;
9   reading a random number within a nonrepeating array of
10 random numbers associated with said position number, wherein
11 said random number corresponds within said array to said
12 selected character; and
13   placing said random number in a position within an
14 encrypted data packet corresponding to said position number.

22.   The method of claim 21, further comprising:
       repeating said steps of selecting a character, reading a
position number, reading a random number corresponding to said
selected character, and placing said random number in a
position corresponding to said position number for each
character within said source data packet to encrypt said
source data packet.

23.   The method of claim 22, further comprising:
       after encrypting said source data packet, encrypting an
authentication code; and
       placing the encrypted authentication code within said
encrypted data packet.

24.   The method of claim 22, further comprising:
       after encrypting said source data packet, encrypting a
stop code; and
       placing the encrypted stop code within said encrypted
data packet.

1   25.   A method of decoding data packets encrypted using a one-
2   time pad, comprising:
3   reading a position number within a randomly ordered,
4   nonrepeating sequence of N numbers within the range of 1 to N;
5   reading a random number located within an encrypted data
6   packet at a position corresponding to said position number;
7   determining a character corresponding to said random
8   number within a nonrepeating array of random numbers
9   associated with said position number; and
10   placing said character in a next available position
11   within a decoded data packet.

1   26.   The method of claim 25, further comprising:
2   repeating said steps of reading a position number,
3   reading a random number, determining a character corresponding
4   to said random number, and placing said character in a next
5   available position for each character in said decoded data
6   packet.

1   27.   The method of claim 26, further comprising:
2   detecting a stop code encrypted in said encrypted data
3   packet.

1   28.   The method of claim 26, further comprising:
2   decoding an authentication code encrypted in said
3   encrypted data packet.

1   29.   A computer program product for use with a data processing
2   system, comprising:
3   a computer usable medium;
4   first instructions on said computer usable medium for
5   selecting a character within a source data packet;

second instructions on said computer usable medium for reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N, wherein said position number is at a location within said sequence corresponding to a location of said selected character within said source data packet;

third instructions on said computer usable medium for reading a random number within a nonrepeating array of random numbers associated with said position number, wherein said random number corresponds within said array to said selected character; and

fourth instructions on said computer usable medium for placing said random number in a position within an encrypted data packet corresponding to said position number.

30. A computer program product for use with a data processing system, comprising:

a computer usable medium;

first instructions on said computer usable medium for reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N;

second instructions on said computer usable medium for reading a random number located within an encrypted data packet at a position corresponding to said position number;

third instructions on said computer usable medium for determining a character corresponding to said random number within a nonrepeating array of random numbers associated with said position number; and

fourth instructions on said computer usable medium for placing said character in a next available position within a decoded data packet.

ABSTRACT OF THE DISCLOSURE
SECURE ENCRYPTION OF DATA PACKETS FOR TRANSMISSION OVER UNSECURE NETWORKS

Pure random numbers from a sheet within a one-time pad are employed to encrypt the bytes of a source data packet and to order the encrypted bytes in a random order within the encrypted data packet. Pure random numbers fill remaining positions within the encrypted data packet. The resulting encrypted data packet is unconditionally secure (i.e., unbreakable). Sheets within the one-time pad are utilized only once, and the one-time pad is replaced when exhausted. For electronic checking applications, the one-time pad is distributed to the user stored in an electronic checkbook, with a copy retained by the bank. For cellular telephone applications, the one-time pad is stored in a replaceable memory chip within the mobile unit with a copy retained at a single, secured central computer. For client-server applications or applications involving sales over the Internet, the one-time pad may be provided to the user on a floppy disk or CD-ROM, with a copy retained by the vendor.

5

10

15

20

102

104

106

Figure 1

206   104

202 →

	206				
	3	14	9	59	79
0=	24	87	42	78	17
1=	92	69	29	96	65
2=	12	67	21	76	82
3=	83	29	38	92	22
4=	28	97	32	79	12
5=	20	75	2	57	15
6=	5	1	50	10	77
7=	63	53	36	35	48
8=	19	42	91	24	30
9=	9	91	90	19	99
*=	45	36	54	63	16

208

. . .

204

Figure 2

302 →

1	2	3	4	5	6	7	*	8	9	0	1	2	3	4	5	6	*	9	7	8	6	0

304 →

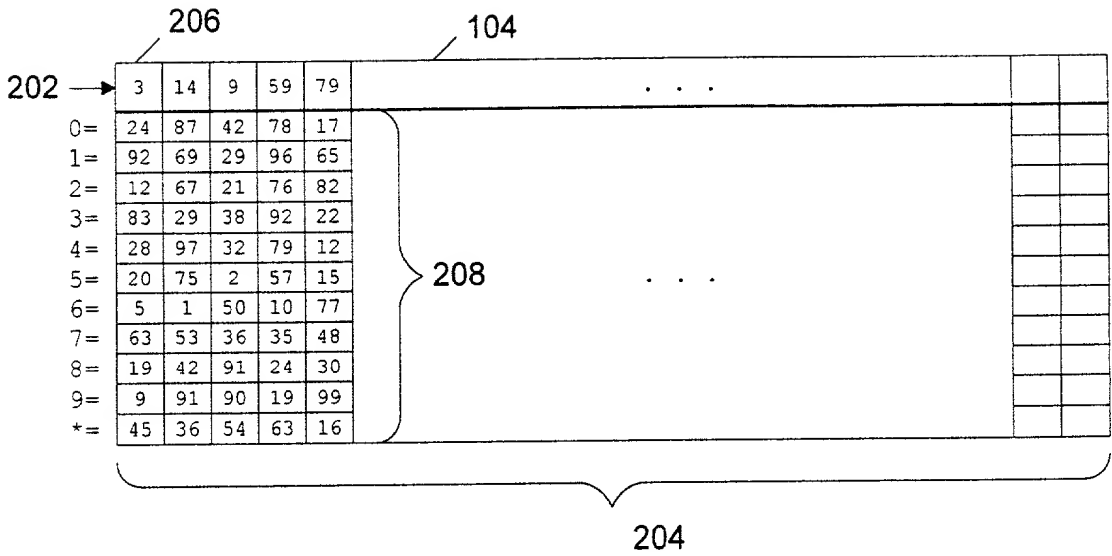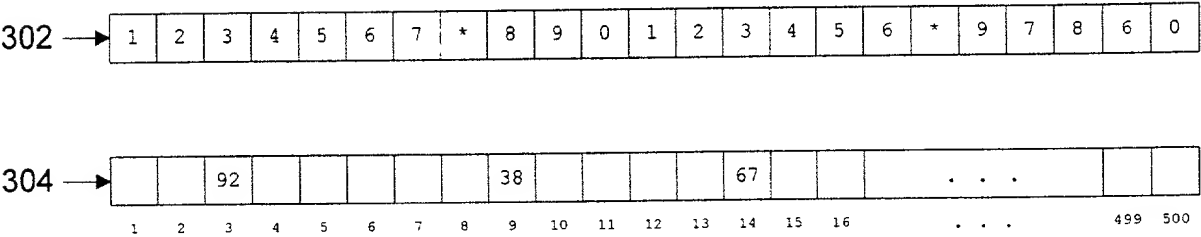|	92					38				67		. . .		
1	2 3	4	5	6	7 8	9	10	11	12 13	14	15 16	. . .	499	500

Figure 3

Figure 4

Figure 5

614

602

Electronic
Checkbook

Receiving
Device

606

608

Internet

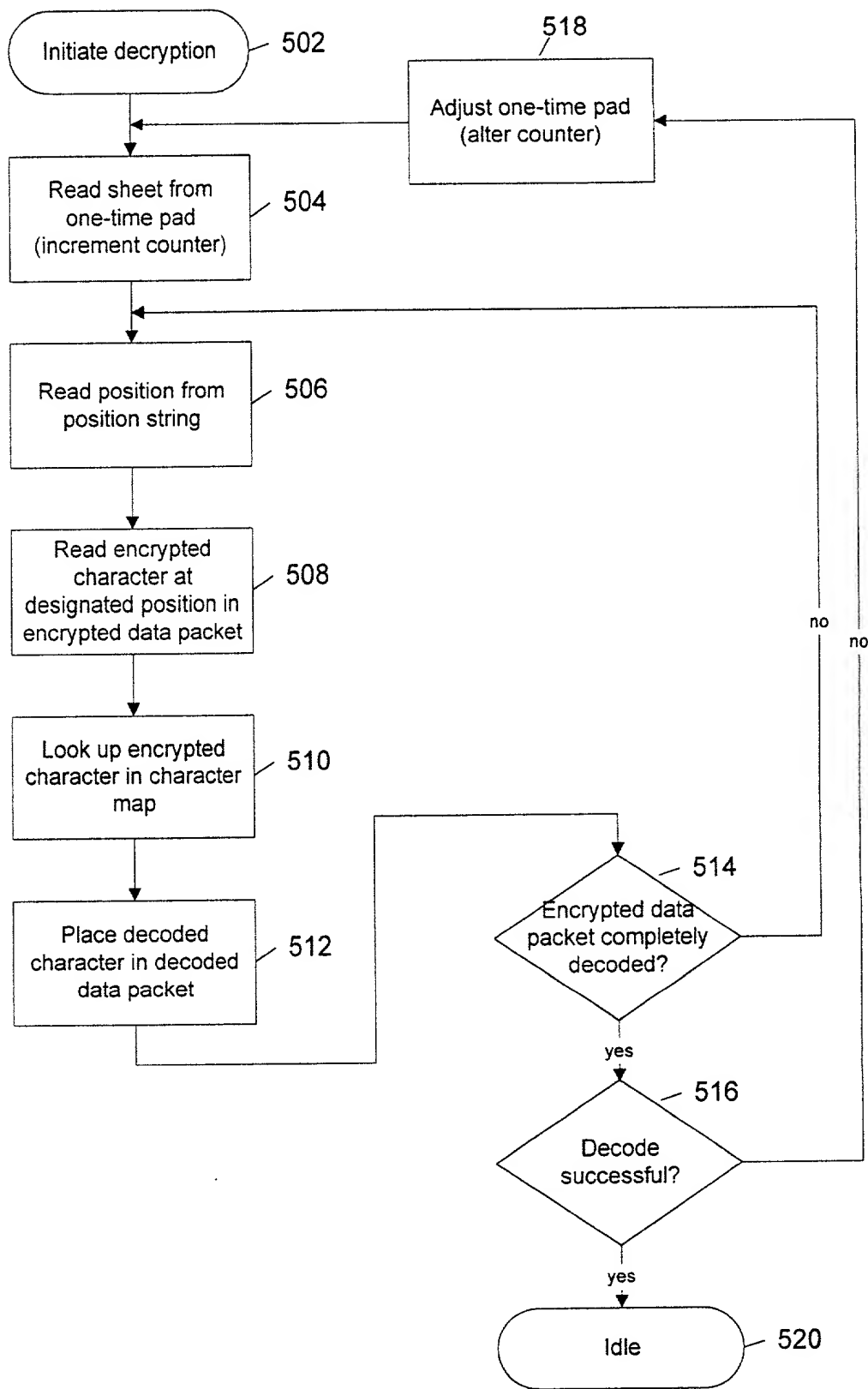612

620

610

624

618

616

SD

604

622
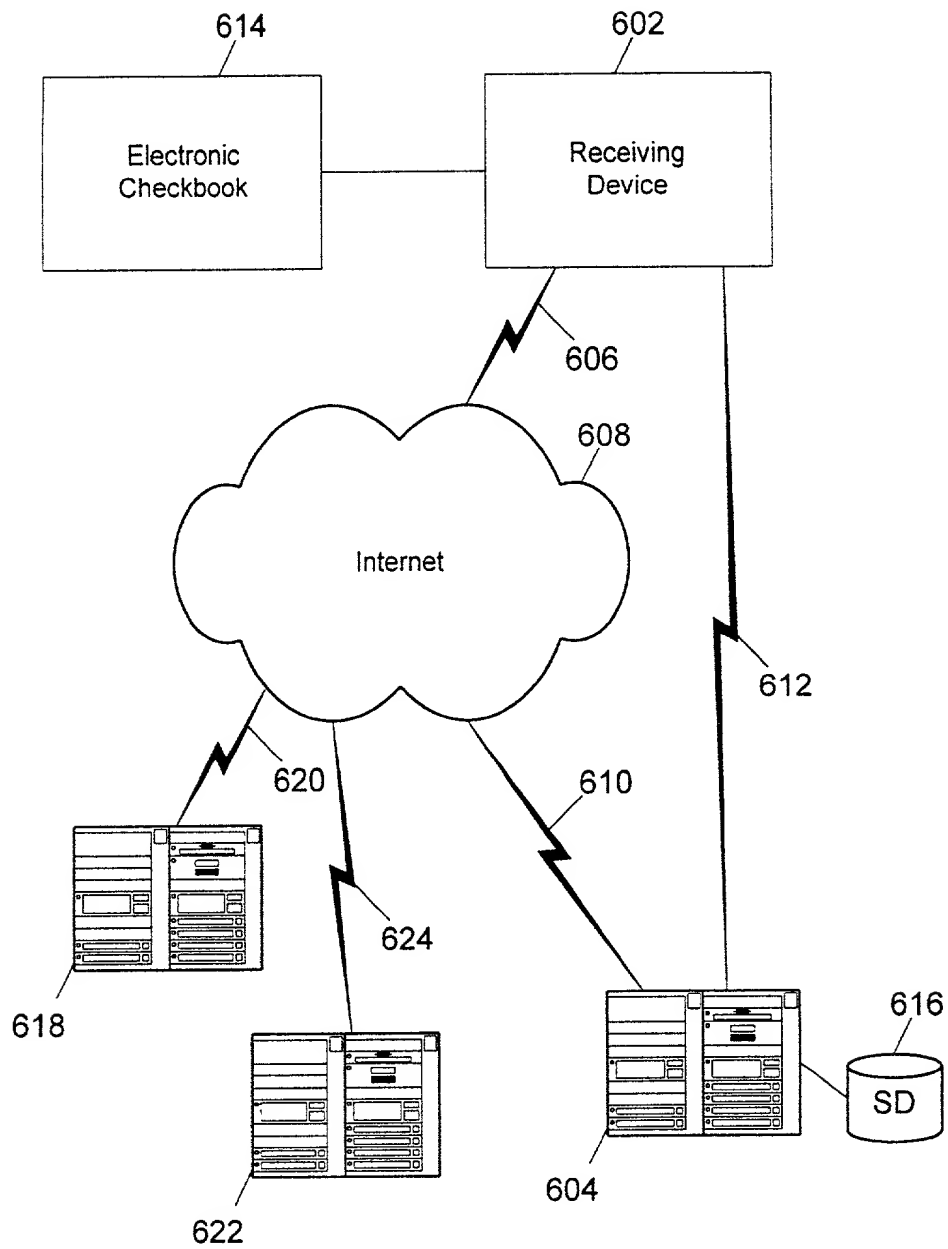
Figure 6

Figure 7

Figure 8

902

User Unit

906

904

Internet

910

908
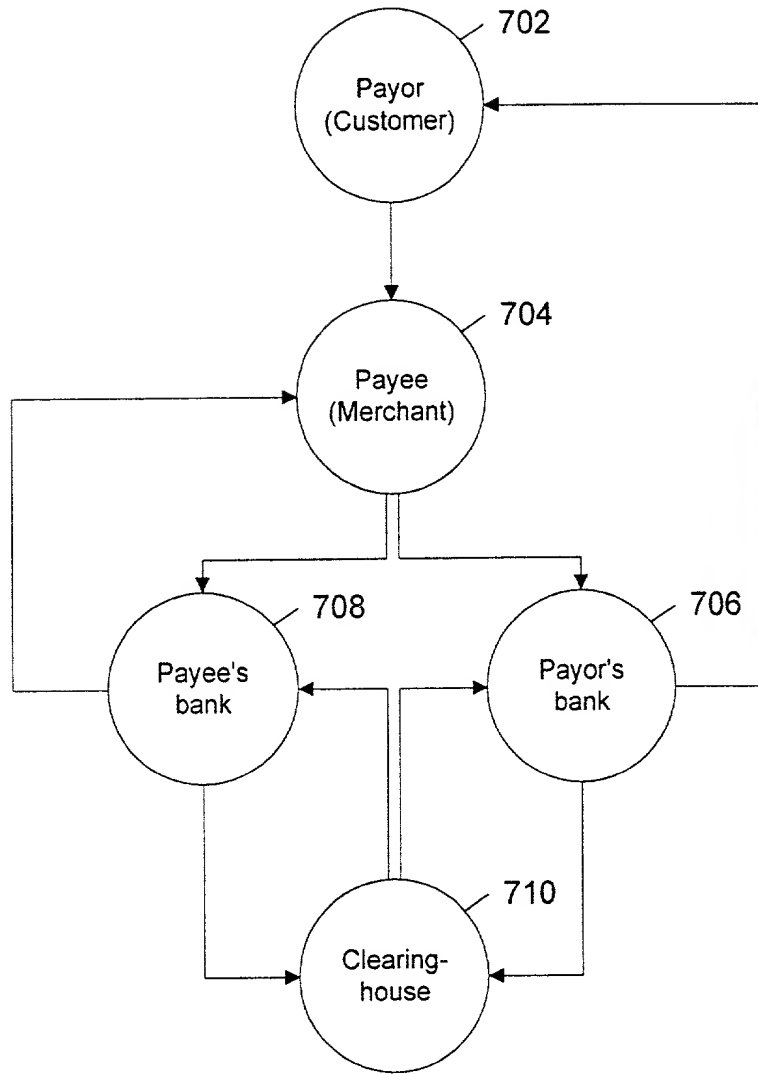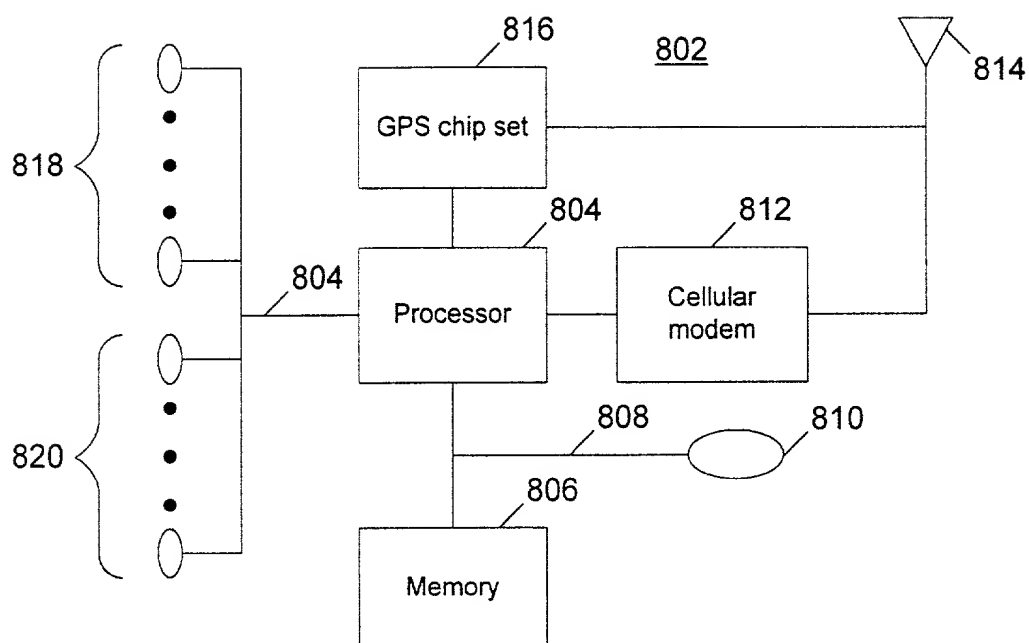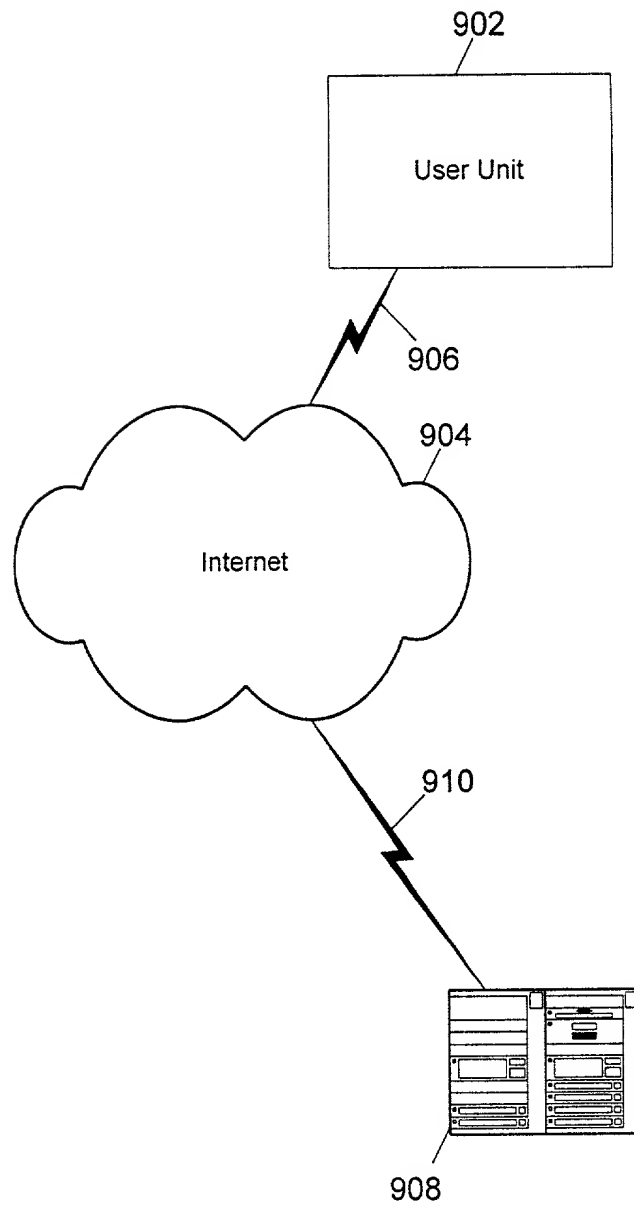
Figure 9

DECLARATION AND POWER OF ATTORNEY FOR

PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name:

I believe I am an original, first and sole inventor (if only one name is listed below) or and original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SECURE ENCRYPTION OF DATA PACKETS FOR TRANSMISSION OVER UNSECURED NETWORKS

the specification of which (check one)
XX_____ is attached hereto
_____ was filed on _____
          as Application Serial No. _____
          and was amended on _____
                                    (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):   Priority Claimed

                                                                    ____ Yes ____ No
_____ _____ _____
      (Number)   (Country)   (Day/Month/Year)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ _____ _____
(Application Serial No.)   (Filing Date)   (Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John W. Henderson, Jr., Reg. No. 26,907; James H. Barksdale, Reg. No. 24,091; Thomas E. Tyson, Reg. No. 28,543; Robert M. Carwell, Reg. No. 28,499; Mark E. McBurney, Reg. No. 33,114; Jeffrey S. LaBaw, Reg. No. 31,633; Douglas H. Lefeve, Reg. No. 26,193; Mark S. Walker, Reg. No. 30,699; Casimer K. Salys, Reg. No. 28,900; Michael A. Davis, Jr., Reg. No. 35,488; David A. Mims, Jr., Reg. No. 32,708; Richard A. Henkler, Reg. No. 39,220; Anthony V. England, Reg. No. 35,129; Volel Emile, Reg. No. 39,969; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond Jr., Reg. No. 18,753; Andrew J. Dillon, Reg. No. 29,634; Kenneth C. Hill, Reg. No. 29,650; Melvin A. Hunn, Reg. No. 32,574; Duke W. Yee, Reg. No. 34,285; Max A. Ciccarelli, Reg. No. 39,454; Jack V. Musgrove, Reg. No. 31,986; Brian F. Russell, Reg. No. 40,796; Daniel E. Venglarik, Reg. No. 39,409; and Alan L. Carlson. Reg. No. 40,939.

Send Correspondence to: Andrew J. Dillon
FELSMAN, BRADLEY, GUNTER & DILLON, L.L.P.
Suite 350 Arboretum Point
9505 Arboretum Blvd.
Austin, Texas 78759

FULL NAME OF FIRST INVENTOR: Ronald Roscoe Bush

INVENTORS SIGNATURE: _____ DATE: August 5, 1997

RESIDENCE: 8645 Piney Creek Bend
Austin, TX 78745

CITIZENSHIP: U.S.

POST OFFICE ADDRESS: Same